

# Architecting Systems for Human Space Flight

Gerald Wocken  
Boeing Space and Communications  
Huntsville, AL

International Space Station  
Payload Display Review Team

(256) 961-2154  
[gerald.f.wocken@boeing.com](mailto:gerald.f.wocken@boeing.com)

## ABSTRACT

Human-system interactions have been largely overlooked in the traditional systems engineering process. Awareness of human factors (HF) has increased in the past few years, but the involvement of HF specialists is still often too little and too late. In systems involving long-duration human space flight, it is essential that the human component be properly considered in the initial architectural definition phase, as well as throughout the system design process. HF analysis must include not only the strengths and limitations of humans in general, but the variability between individuals and within an individual over time, and the dynamics of group interactions.

## INTRODUCTION

Systems intended for human space flight have often been functional extensions of ground-based systems, with the hardware modified for the space environment. Even when systems have been developed from the start with the space (microgravity, radiation, vacuum, meteoroid, etc.) environment in mind, the human component has often been added as an afterthought. For missions measured in days, the resulting need for the crew to accommodate the hardware has been an acceptable inconvenience.

As longer-duration space flights become a reality, there will be an increased need to consider the human component and its interfaces as integral parts of the architecture from the beginning of the process. Hardships that might be considered part of the adventure for a short mission can become serious irritations when they continue for months or years, and adversely affect crew and system performance.

A search of the 1990-2000 INCOSE Symposium database (350 pages of abstracts) discovered less than a dozen papers containing either the word 'human' or 'space'. Almost all of the papers on Human Factors addressed the issue of how HF needs to be included in the SE process, with the implication, if not the expressed statement, that HF was not being properly considered. The space-related papers were almost all on robotic space systems, and if they considered the human element at all, it was with regard to the design team or the ground controllers of the mission.

## TRADITIONAL APPROACH TO HUMAN SPACE FLIGHT SYSTEMS

The traditional approach to human-machine systems generally results in systems that fail to meet their performance specifications, and require the customer to delay acceptance and delivery, accept the system limitations until they can be fixed, or increase the number or qualifications of personnel needed for operations. (MacLeod) The fire detection and suppression (FDS) system for the Space Station is an example of the traditional approach. In the late 1980's it was recognized that a fire in space might be difficult to detect, and the results could be catastrophic. If it became necessary to abandon the station there would be only one 'lifeboat', and the fire might cut the crew off from it.

The original FDS system architects used the model of a terrestrial building system, modified for the microgravity environment. Instead of a tank of water on the roof, tanks of pressurized inert gas were used. Instead of heat-sensitive passive fusible plugs, electro-optical smoke and flame detectors and a maze of 'avionics air' ducts were used. Instead of sprinkler heads in each room, valves with diffusing nozzles were provided in each rack, standoff, and other volume where a fire could occur. Networks of pipes and wires more complex than those used in most ground facilities connected the components to each other and to controlling computers.

CO<sub>2</sub> was selected as the suppressant (other agents were toxic, corrosive, and/or could not be removed by onboard air cleaning equipment). Each tank had multiple pressure sensors and outlet valves, to prevent the inadvertent leakage of CO<sub>2</sub> into the station, or overpressure that might result in tank rupture. Actively commanded normally-open valves were needed at the end of each pipe to control the CO<sub>2</sub> flow, because it might not be possible to command a closed valve in the fire area to open, if the wiring was damaged. Since smoke doesn't rise or spread much in microgravity, a constantly moving airflow (fans and ducts) had to be provided through every potential fire volume to carry any combustion products to the associated smoke detector. The smoke detectors each included redundant sensors, a microprocessor, and a communications interface. Redundant copies of the FDS software had to be running on different computers, in case the fire occurred in a computer rack. Every problem that was found was solvable, but every solution brought new problems (unintended consequences) and increased system complexity. The system's designers found themselves in a hole, and tried to solve the problem by digging harder.

If a smoke or flame detector identified a fire, it would run an internal self-diagnostic routine, and then, if it confirmed the fire, it would notify the computer system, which would sound an alarm, close the CO<sub>2</sub> valves not in the fire area, shut down all air flow to the affected part of the station, cut off electrical power to the area, and open the valves on one of the main CO<sub>2</sub> tanks. The crew would leave the affected module and seal it off until the fire was out and the cabin air restored to breathable quality (a period of at least several hours, or considerably longer if the atmosphere had to be dumped overboard). Then they would try to recover the data and systems that would have been lost during the emergency shutdown. The used CO<sub>2</sub> tank would be replaced on the earliest possible resupply flight. The FDS system consumed a significant, and increasing, portion of the station's scarce resources (weight, space, and computing and electrical power), and did not involve the crew at all, until after the emergency was over. Although the presence of a human crew was the driving force behind having an FDS system, they were not part of its architecture.

Eventually, the team recognized that it was time to stop digging, and take a look at the situation. If a fire started in still air in microgravity, it would likely either smother itself in its own smoke, or spread very slowly, in a more-or-less spherical manner. In either case, it would almost certainly cause a detectable failure of the equipment in which it occurred long before impacting anything else. The presence of a constant airflow would both feed and spread the fire. The CO<sub>2</sub> distribution plumbing would contain a large volume of air, all of which would be blown across the flame before the CO<sub>2</sub> reached it, fanning it farther (even if the system worked as designed). The complexity of both the detection and suppression subsystems made some failure highly likely, and the consequences of a false alarm would probably be as bad as those of an actual fire. The need for directed airflow through and around every component in every rack would also severely constrain rack packaging.

By the mid 1990's, reductions in Space Station resources made the FDS architecture, as it had evolved, untenable. A clean-sheet approach to FDS design considered the physics of microgravity combustion and the capabilities of the crew, and reduced the weight, volume, and resource needs of the system by 90 percent, while making the human component an integral part of the architecture. Each potential fire volume is now isolated from the rest of the station, and has a fire extinguisher hole in its front panel. A portable CO<sub>2</sub> extinguisher is located at each end of each module. Only those few racks that require forced-air cooling (most are water-cooled) have smoke detectors. Other detectors are located in the air conditioning return ducts, to indicate if smoke is somewhere in the cabin. If a component failure indicates that a fire might exist, or smoke is detected, the computer system alerts the crew so they can look for other symptoms to verify and localize it, and take appropriate action. The smaller amount of CO<sub>2</sub> in the portable extinguishers does not require that the crew evacuate the module in most cases.

## HUMAN FACTORS ACCEPTANCE

A decade ago, HF was the ugly stepchild in the systems engineering family. HF engineers were lucky to be acknowledged, much less respected. In 1995, Buie & Vallone stated "As currently defined and practiced, the systems engineering process overlooks the design of human-system interaction as a systems engineering activity." According to MacLeod, "HF input into the design process occurs rather late in the design life cycle precluding any major HF influence in the all-important early design processes. Moreover, the traditional and late use of Ergonomists results in some cases of their derogatory and fruitless naming as 'flower arrangers'. This term in popular use in the UK aircraft industry ... "

A comparison of the 1990 and 1998 editions of Blanchard & Fabrycky shows how the acceptance of the HF specialty has improved, at least in academia, if not yet in practice. In the second edition, the human factors chapter (called Design for Manability) is 24 pages long, with 5 subsections; in the third edition, the chapter (now called Design for Usability) is 30 pages long, with 7 subsections, and significantly more coverage of HF is incorporated into the general systems engineering process sections. The subsection on psychological factors is 450 percent larger in the later edition.

The subsection on 'error analysis' in the second edition listed, as possible causes: failure to comply with procedures, failure to obtain necessary data, failure to read displays correctly,

failure to operate controls properly, and failure to monitor and respond to changes; i.e., problems were blamed on the crew. In the third edition, the possible causes of errors listed were: inadequate workspace layout, inadequate facilities, inadequate lighting temperature and sound levels, inadequate displays, inadequate training, inadequate management (communications and planning), and inadequate procedures and job aids; i.e., the responsibility is placed on the system's designers, not its users.

The second edition said, "One of the major objectives in system design is to minimize, if not eliminate, the possibility of introducing human error ... The primary source of failures is the human being." (p. 454). The third edition (p. 482) deleted these misanthropic statements completely. The authors now seem to have developed an appreciation for the human component of systems as something to be nurtured rather than feared.

Within the past 5 years, the U.S. Army (MANPRINT) and the British Ministry of Defence have begun encouraging their contractors to integrate HF into the systems engineering process (Ward & Harmer). These efforts, however, are still limited to the highest levels of the culture and process.

## **COGNITIVE FUNCTION ALLOCATION**

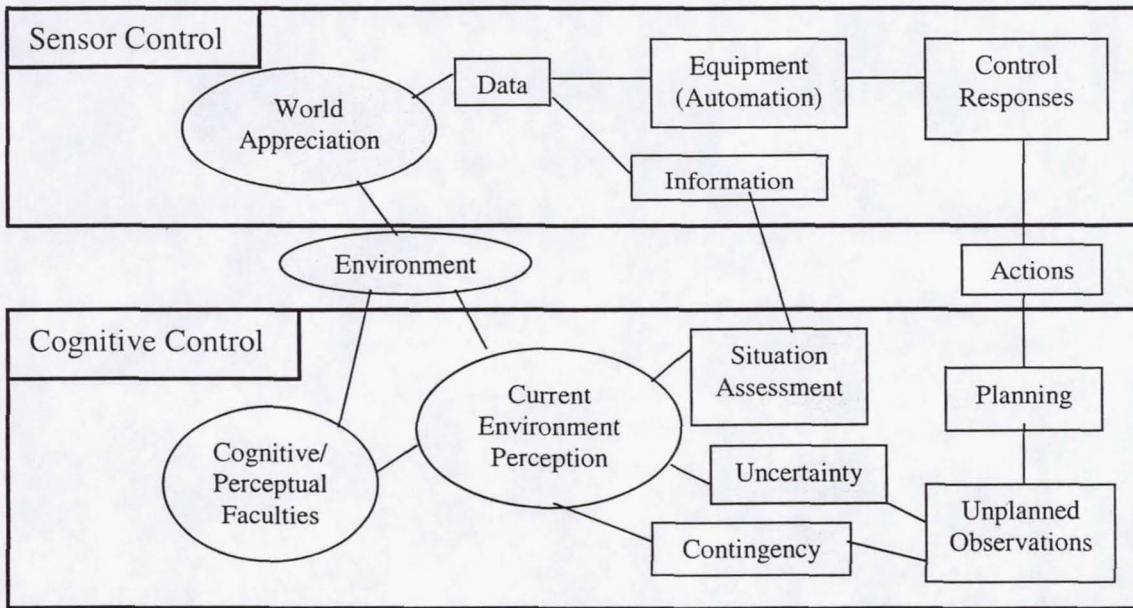
A system specification should encompass the totality of human-machine system functional requirements and performance. The human operator is mainly considered by engineering processes to be a constraint on system design, without associated performance requirements. (MacLeod)

System related cognitive functions are associated with the assessment and understanding of the work environment, system control and direction, system management, supervision of system task performance, and teamwork. Such functions have traditionally been assigned to the human component, in support of required system performance. Any improved approach must include the specification of system performance covering cognitive functions that may be allocated to engineered (non-human) components of the system where appropriate.

Traditional application of HF (man is better at ... , machine is better at ...) fails to consider individual differences and the complementary nature of the contributions of man and machine to system performance. HF input also generally occurs late in the development process, by which time all of the available alternatives may be fundamentally flawed. Human functionality should be addressed from the outset of system design so that human influences can be more readily considered during the physical design of the system.

The term 'cognition' can apply to functions and tasks resident in both man and machine. The cognitive function refers to the translation of intended tasks into activities. The essential role of cognitive functions is in maintaining stable system control. They represent a focused understanding of the state of system performance with relation to system work goals. The greater the degree of system automation, the greater becomes the importance of system feedback to the operator.

Functional specifications must capture the necessary cognitive functions required by the system, not the specific capabilities of the human operator. The specified cognitive functions might reside in the engineered system, the operator, or both. Functional allocation would be mainly an allocation of levels of control, considering the degree of automation and the feedback needs of the human in command of the system. The following figure shows a model of a human-machine system. The lines are shown without arrowheads since, in most cases, information flow can be in either direction.



Human-Machine System Functional Classification

The evolution of functional assignments is illustrated by the history of aircraft stall indicators. In early airplanes, the pilot was responsible for both sensory and cognitive functions, as he watched a piece of ribbon tied to a strut and took appropriate action. By mid-century, the machine had taken over the sensing functions, displaying airspeed and angle of attack on the instrument panel, while the pilot still decided what to do about it. On current aircraft, the machine performs the cognitive functions of situation assessment and advice in addition to sensing, and tells the crew what to do via a 'stick shaker' and/or voice instructions.

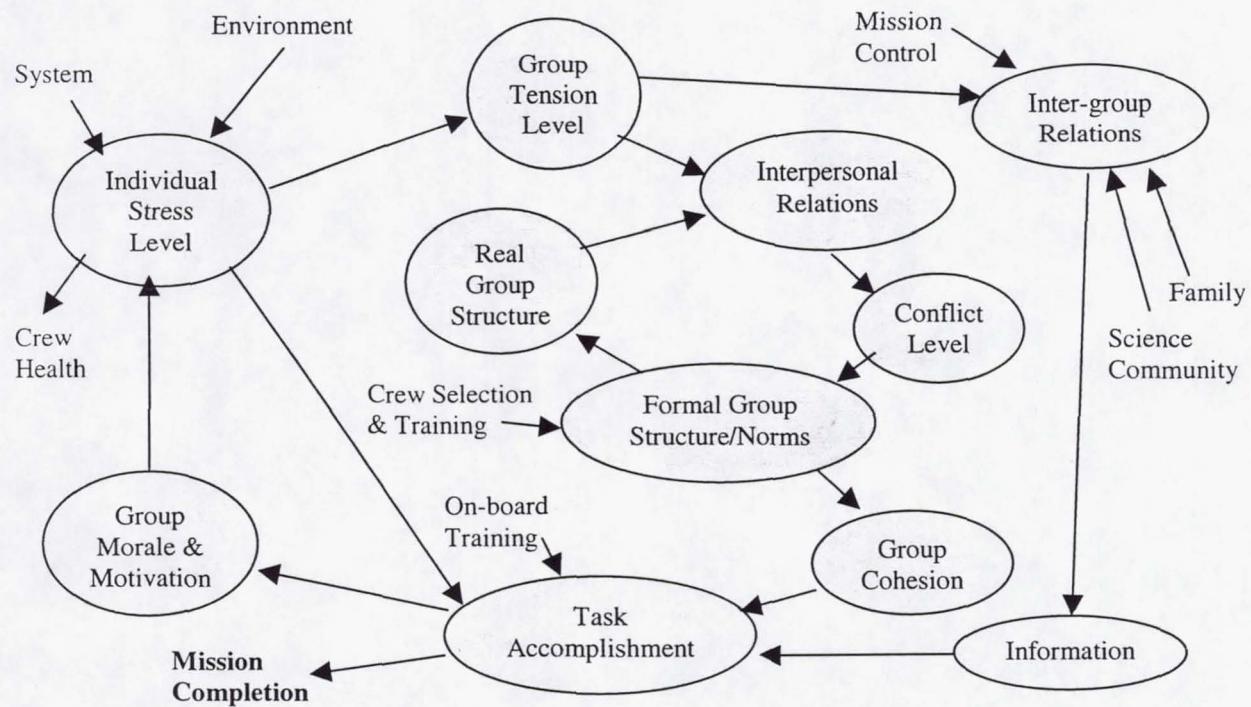
## GROUP DYNAMICS

The spacecraft and its crew constitute a single dynamic system, in which the components are integrated by the flow of materials, manpower, and information. Other forces that can affect system performance include those originating within the individual crewmembers, at the group level, imposed by the system hardware and software, or imposed by the environment.

An accurate statement and prediction of causal relationships for crew behavior is very difficult, as evidenced by the many theories put forth by psychologists and sociologists. Most theories of

human behavior are based on a static view, although dynamic interactions are the most important factor. (Upshaw)

The Crew-System Interactions Model shown below relates the various system parameters affecting the crew in such a way that the situational variability of the crew interactions is accounted for. Although it is only an analytical model, it can provide insights into the functioning of the real system to help identify desirable crew norms and standards to ensure that mission objectives are met.



Crew-System Interactions Model

The uncensored daily Space Station logs that NASA formerly posted on the Internet provided insight into the everyday working of the station, and some of the human interactions that occur. Many of the entries indicate the crew's irritation with the software provided to them: "We are able to log in, but the program either locks up or won't launch when we try to run it", and "We are getting blocked from changing the printer job cue [sic]. Apparently we don't have the right permissions." After spending half a day seeking a storage bag that should have been found in two minutes, the station commander complained that the inventory management system database had been corrupted by bad data from mission controllers on Earth. In another passage, he scolded the two flight control centers (Houston and Moscow) for not seeing the Space Station as "more of a unified environment."

## **OTHER FACTORS AFFECTING HUMAN SPACE FLIGHT**

Prolonged exposure to cosmic rays may damage regions of the brain responsible for cognition, decision-making and language comprehension. This represents a significant danger when a trip to Mars is expected to take six to ten months – each way, and visits to the outer planets much longer. These effects are in addition to the restlessness, anxiety, sleep disturbances, disorientation, anger, and decreased performance that result from long term isolation in any environment (e.g., cabin fever). If any of the crew experiences these symptoms, it could endanger the entire crew and the mission.

A computer system that could remotely monitor the cognitive functioning of astronauts by using acoustic measures of their speech would allow NASA to respond to changes during a mission. Brown University recently received a NASA grant to develop a system to monitor the cognitive abilities of astronauts during a proposed manned mission to Mars in 2020. The research project is based on new insights into how brains work. Complex acts such as understanding the meaning of a sentence, reaching a decision or planning ahead involve activity in many parts of the brain, including the basal ganglia.

While such a crew monitoring system could provide useful advice on the capabilities of the human crew, it is unlikely that it will be completely trusted, at least any time soon. Computer problems continue to be the major operational difficulties for both manned and unmanned space vehicles. Ground control centers would have to have override control for situations where the computers and the crew each judged the other to be cognitively impaired. System architectures will have to allow for the degradation of the capabilities of both silicon-based and carbon-based cognitive system components.

## **CONCLUSIONS**

A comprehensive approach to architecting human space flight systems must consider all elements in the system and their interactions from the beginning, and allocate functions where they can best be performed. The architecting process should start with a clear mission statement, followed by a thorough understanding of the operations concept, the functions to be performed, and the environment in which the system will operate. Based on this knowledge, the architecture can be defined, with the appropriate functions allocated to the vehicle, crew, hardware, and software. Since “To err is human ...”, failure modes and effects analysis must give the same consideration to potential human errors as to hardware or software failures. It must be assumed that the crew will make mistakes, in spite of any efforts to minimize or eliminate them.

The traditional paradigm of man/machine systems should be replaced with one that allocates functions based on whether they are more cognitive or mechanistic, with the cognitive functions divided between human and engineered components. Mechanistic functions could be automated, with provision for contingency override. Routine cognitive functions could be automated with human oversight. Advisory functions would be automated, but would require human concurrence. Adaptive software would be able to assume increased responsibility as its

experience level increased, but the human element (on-board and/or on Earth) must retain the final decision authority and responsibility for policy interpretation.

The human environment includes adaptation to inter- and intra-group dynamics. System architectures must include man-man as well as man-machine interfaces. Forces acting both within and between the components and the external environment affect the system's performance. As the distance from Earth increases, the level of autonomous operation of the integrated spacecraft system also increases. This will likely lead to an increase in group cohesion (with the accompanying risk of groupthink) and less dependence on ground controllers.

For long-duration missions, training will have to be built into the system architecture. The limits of human memory will prevent training to the same level of intensity as a Shuttle mission, while the total number of tasks will be much greater. An on-board continuous education program will have to be part of the system if the crew are to have the skill proficiency levels needed at each phase of the mission. Accurate mental models provide useful knowledge of system operations when learned procedures fail, especially in emergency situations. The training process will have to form the crew's different mental models into ones that are at least compatible, if not identical.

One way to implement the man-machine allocation of functions would be to define an 'electronic crewman' as part of the system architecture, to serve as a repository for those cognitive functions assigned to the machine.

The change from the traditional technology-centered approach to a more human-centered systems engineering process, where the needs, capabilities, and limitations of the human element become key design drivers, will require credible and long-term commitment from academia, government and industry. The steps taken to date are more a statement of intentions than an accomplished transformation -- a good beginning, but they will not have a lasting effect by themselves. Future architectures for long-duration manned space flight systems must recognize the mutual interdependence of the automated systems and the crew.